

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,335	07/05/2001	Peter Bernhard Kaars	US018099	5618

7590

08/18/2004

Corporate Patent Counsel
U.S. Philips Corporation
580 White Plains Road
Tarrytown, NY 10591

EXAMINER

CHEA, PHILIP J

ART UNIT

PAPER NUMBER

2153

DATE MAILED: 08/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

RECEIVED

AUG 25 2004

Technology Center 2100

Office Action Summary

Application No.

09/900,335

Applicant(s)

KAARS, PETER BERNHARD

Examiner

Philip J Chea

Art Unit

2153

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 7/5/2001.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-8 have been examined.

Priority

2. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows:

An application in which the benefits of an earlier application are desired must contain a specific reference to the prior application(s) in the first sentence of the specification or in an application data sheet (37 CFR 1.78(a)(2) and (a)(5)). The specific reference to any prior nonprovisional application must include the relationship (i.e., continuation, divisional, or continuation-in-part) between the applications except when the reference is to a prior application of a CPA assigned the same application number.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on July 5, 2001 was filed after the mailing date of the 5th on July 2001. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

4. The abstract of the disclosure is objected to because:
 - Note, the heading of the abstract should be "Abstract of the Disclosure".
 - Note line 1, a paragraph indentation should be included.
 - Note line 2, a period after network should be included.

Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because of the following informalities:

Art Unit: 2153

- Note page 3, lines 2 and 6, "analyses", and page 4, paragraph 14, line 5, "analyzes", consistent language should be used.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 7 and 8 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 7 and 8 refer to software that does not reside on a computer readable medium.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 7, and 8 rejected under 35 U.S.C. 102(e) as being anticipated by Ramaley et al. (U.S. 6,687,741).

6-1 As per claims 1, 7, and 8, Ramaley et al. disclose a system of controlling communication of content information from a sender to a receiver via a data network, as claimed, comprising:

- means for verifying if the content information is available from a source other than the sender (column 5, lines 51-64); and

Art Unit: 2153

- means for deciding if the content information is available from the other source, substituting for the content information a pointer to the other source (column 5, lines 51-64).

Claims 7 and 8 are rejected as being software implementing the method as disclosed by Ramaley et al (see rejection above).

6-2 As per claim 2, Ramaley et al. disclose controlling communication content on request of at least the sender (column 6, lines 4-19).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7-1 Claim 3 rejected under 35 U.S.C. 103(a) as being unpatentable over Ramaley et al. as applied to claim 1 above, and further in view of Berghel. Although Ramaley et al. disclose substantial features of the claimed invention (discussed above), he fails to directly disclose verifying the content based on a watermark. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ramaley, as evidenced by Berghel.

In an analogous art, Berghel discloses watermarks being used as a method of authenticating a document for verification purposes (page 2, see WATERMARKS IN USE, line 1), such as claimed above.

Given the teaching of Berghel, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Ramaley et al. by employing a

Art Unit: 2153

verification method based on watermarks, such as disclosed by Berghel, in order to guarantee authenticity, quality, ownership, and source (page 1, see Watermarking Cyberspace, 3rd paragraph). It would have been obvious to use the fingerprinting system taught by Zabetian to verify that a particular document located at another source is the same document from the local source.

7-2 Claims 4-6 rejected under 35 U.S.C. 103(a) as being unpatentable over Ramaley et al. as applied to claim 1 above, and further in view of Zabetian (U.S. 6,327,656).

As per claim 4, although Ramaley et al. disclose substantial features of the claimed invention (discussed above), he fails to directly disclose verifying the content based on a fingerprint of the content. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ramaley, as evidenced by Zabetian.

In an analogous art, Zabetian discloses a system that can receive and transmit electronic mail (column 2, lines 42-45), verifying the document is the one to be received by using a fingerprint (column 7, lines 21-29).

Given the teaching of Zabetian, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Ramaley et al. by employing a fingerprinting method, such as disclosed by Zabetian, in order to identify and distinguish the document from other documents, even one that appear to be similar from one another (column 2, lines 4-9). It would have been obvious to use the fingerprinting system taught by Zabetian to verify that a particular document located at another source is the same document from the local source.

7-3 As per claim 5, although Ramaley et al. disclose substantial features of the claimed invention (discussed above), he fails to directly disclose the communication being carried out depending on the sender being authorized to communicate the content information. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ramaley, as evidenced by Zabetian.

Art Unit: 2153

In an analogous art, Zabetian discloses a system that can receive and transmit electronic mail conditionally being carried out depending on the sender being authorized to communicate the content (column 6, lines 37-53).

Given the teaching of Zabetian, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Ramaley et al. by employing a sender authorization, such as disclosed by Zabetian, in order to certify the content that is being transmitted, and be alerted of any fraudulent activity (column 6, lines 54-62).

7-4 As per claim 6, although Ramaley et al. disclose substantial features of the claimed invention (discussed above), he fails to directly disclose the communication being carried out depending on the receiver being authorized to receive the content. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ramaley, as evidenced by Zabetian.

In an analogous art, Zabetian discloses a system that can receive and transmit electronic mail depending on the receiver being authorized to receive the content information (column 11, lines 17-43).

Given the teaching of Zabetian, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Ramaley et al. by employing a receiver authorization, such as disclosed by Zabetian, in order to confirm the receiver was correctly intended (column 11, lines 53-62).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Kuzma (U.S. 5,771,355)

Kuzma (U.S. 5,781,901)

Beck et al. (U.S. 5,903,723)

Birrell et al. (U.S. 6,009,462).

Art Unit: 2153


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Philip J Chea whose telephone number is 703-605-1202. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton Burgess can be reached on 703-305-4792. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Philip J Chea
Examiner
Art Unit 2153

PJC


GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Form PTO-1449 U.S. DEPARTMENT OF COMMERCE (REV. 7-80) PATENT AND TRADEMARK OFFICE				Atty. Docket No. US018099		Serial No.	
INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)				Applicant: Peter Bernhard Kaars			
				Filing Date		Group	

JES79 U.S. PTO
 09/900335
 04/05/01

U.S. PATENT DOCUMENTS									
Ex. Int.	Document Number	Date	Name	Class	Sub-class	Filing Date If Approp.			
	AA								
	AB								
	AC								
	AD								
	AE								
	AF								
	AF								

FOREIGN PATENT DOCUMENTS									
	Document Number	Date	Country	Class	Sub-Class	Trans.			
						Yes	No		
	AG								
	AH								
	AI								
	AJ								
	AK								

OTHER (Including Author, Title, Date, Pertinent Pages, Etc.)	
AL	US S/N 09/642,713 (US000213) "Selective Sending of Portions of Electronic Content"
AM	US S/N 09/374,694 (PHA23737) "Semantic Caching"
AN	US S/N 09/844,570 (US018052) "Distributed Storage on a P2P Network Architecture"
AO	
AP	
AQ	

Examiner <u>PHILIP CHEA</u>	Date Considered <u>7/27/04</u>
-----------------------------	--------------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include a Copy of this form with next communication to applicant.

Notice of References Cited	Application/Control No. 09/900,335	Applicant(s)/Patent Under Reexamination KAARS, PETER BERNHARD	
	Examiner Philip J Chea	Art Unit 2153	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,771,355	06-1998	Kuzma, Andrew J.	709/232
	B	US-5,903,723	05-1999	Beck et al.	709/200
	C	US-5,903,892	05-1999	Hoffert et al.	707/10
	D	US-6,009,462	12-1999	Birrell et al.	709/206
	E	US-6,275,848	08-2001	Arnold, Gordon K.	709/206
	F	US-6,327,656	12-2001	Zabetian, Mahboud	713/176
	G	US-6,687,741	02-2004	Ramaley et al.	709/206
	H	US-5,781,901	07-1998	Kuzma, Andrew J.	707/10
	I	US-5,790,790	08-1998	Smith et al.	709/206
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Berghel, Hal. "Digital Village." 1997. 27 Jul. 2004 < http://www.acm.org/~hlb/col-edit/digital_village/nov_97/dv_11-97.html >.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



copyright notice

2101

accesses since August 30, 1997

Hal Berghel's *Digital Village*....

Watermarking Cyberspace

The use of watermarks is almost as old as paper manufacturing. Ancients poured their "half-stuff" slurry of fiber and water onto mesh molds to collect the fiber, then dispersed the slurry within "deckle" frames to add shape and uniformity, and finally applied great pressure to expel the water and cohere the fiber. This process hasn't changed too terribly much in 2,000 years, even with the benefit of automation. One byproduct of this process is the watermark - the technique of impressing into the paper a form, image or text derived from the "negative" in the mold, as the paper fibers are squeezed and dried.

Paper watermarks have been in wide use since the late middle ages. Their earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock. In more recent times, watermarks have also been used to certify the composition of the paper, including the nature of the fibers used. Today, most developed countries also watermark their paper currencies and postage stamps to make forgery more difficult.

The digitization of our world expanded our concept of watermark to include immaterial, digital impressions for use in authenticating ownership claims and protecting proprietary interests. However, in principle, digital watermarks are not unlike their paper ancestors. They signify something about the token of a document or file in which they inhere. Whether the product of a Fourdrinier paper press or a discrete cosine transformation, watermarks of varying degrees of visibility are added to presentation media as a guarantee of authenticity, quality, ownership, and source.

WATERMARKS IN CONTEXT

A digital watermark is a digital signal or pattern inserted into a digital "document" (e.g., text, graphics, multimedia presentations). As such, it is a form of electronic watermark much like the corporate logos used by the cable television industry to identify the source of the program on screen, typically along the lower periphery of the television screen. Such cable companies, we may assume, feel that the advertising advantage of the ever-present, on-screen logo, together with the legal benefit of having a source signature persist under video recording, more than offset the aggregate user-annoyance and distraction.

Digital watermarks extend these advantages to digital documents. A signal or pattern may be digitally imposed on a document prior to sale or distribution. The persistence of the watermark under transmission, and some common forms of transformation, contribute to our ability to authenticate copies. This, in turn, should enable us to protect our ownership rights in digital information, even in the undisciplined, anarchistic world of the Internet. (see Figure 1)

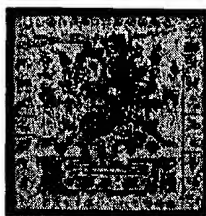


Figure 1. *Digitized copy of artwork from a sixteenth century Aztec manuscript. Note that the circular digital watermark is most visible against light background. Faint watermarks tend to "hide" in the intense, foreground imagery. [Source: IBM's Digital Library Project. Used with permission.]*

Before we get into the detail of what digital watermarking is, we'll first explain what it is not. Digital watermarking is not encryption, which also involves file transformation. It is a common practice nowadays to encrypt digital documents so that they become un-viewable without a decryption key. Unlike encryption, however, digital watermarking leaves the original image or (or file) basically intact and recognizable. Further, decrypted documents are free of any residual effects of encryption, whereas visible digital watermarks are designed to be persistent in viewing, printing, or subsequent re-transmission or dissemination.

Digital watermarking is also to be contrasted with digital fingerprinting, which produces a "meta" file that describes the contents of the source file. Cyclic redundancy checking and checksum algorithms are both simple uses of file fingerprinting for error detection applications. A more advanced use of fingerprinting is to be found in RSA Data Security's use of message digests for authentication purposes. Digests are the result of applying a hashing algorithm (e.g., MD5, SHA) to a document or file to produce an identifying bit string (fingerprint). If the receiver's hash algorithm produces the same message digest for the file as the sender's, the file is authentic. Of course, this assumes that sender and receiver use the same software, hence the same hash algorithm.

Fingerprints may also serve as a digital signatures. If the message digest discussed above were further encrypted, converted to plaintext, and attached to the original file or message in transit, the plaintext version of the message digest (fingerprint) would also serve as a digital signature for the original file. While both fingerprints and signatures accompany unaltered source documents, signatures, like their penned counterparts, are embedded in the document itself even if in encrypted form.

WATERMARKS IN USE

Authentication is but one use of digital watermarking. Both symmetric and asymmetric hashing algorithms can be used to embed a unique digital imprint on a document or file. If the removal of an imprint yields the original document (which is to say that the "stripped" watermark is identical to the embedded watermark), then the copy is authentic. Once again, this assumes that the "stripping" algorithm is available to the end-user. Such authentication techniques are usually associated with some sort of encryption for the distribution of keys, programs, etc. which are related to the watermarked documents.

In addition, watermarks are also used as a check for non-repudiable duplication and transmission. In this

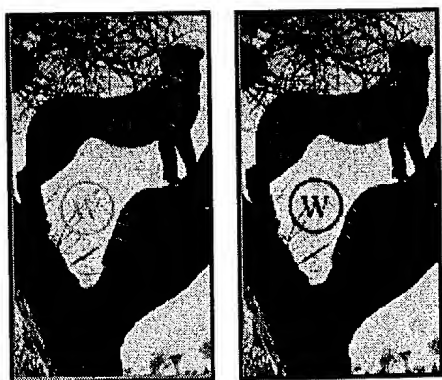
case, the owner, creator or sender imprints a watermark which is unique for each receiver. The watermark holds under subsequent re-transmission, so the "authorized" source of unauthorized copies may be easily identified after extraction. A collateral benefit is that the intended recipient of a document token could always be identified.

However, these applications really only apply to the class of invisible watermarks. Visible watermarks (as in Figure 1) contribute to document and transmission security in different ways. To illustrate, visible watermarks are more overt means of discouraging theft and unauthorized use both by reducing the commercial value of a document and making it obvious to the criminally inclined that the document's ownership has been definitively established. We observe that invisible watermarks only have this effect if the digital thief is aware of the technology and the possibility that watermarks may be present on a document of interest.

There are several characteristics of effective watermarks. For one, they must be difficult or impossible to remove. For another, they must survive common document modifications and transformations (e.g., cropping and compressing image files). Third, they must, in principle at least, be easily detectable and removable by authorized users with such privileges (e.g., law enforcement agencies). Invisible watermarks should also be imperceptible, while visible watermarks should be perceptible enough to discourage theft but not perceptible enough to decrease the utility or appreciation of the document.

WATERMARKING PRACTICE

Watermarking techniques tend to divide into two categories, text and image, according to the type of document to be watermarked. In the case of imagery, several different methods enable watermarking in the spatial domain from simply flipping low-order bits of selected pixels to superimposing watermark symbols over an area of a graphic. Spatial domain watermarking is illustrated in Figures 2a and 2b that demonstrate how the degree of visibility of the watermark depends upon its intensity and the nature of the background.



Figures Figures 2a and 2b. *Two (of many) Two watermarked images identical but for the intensity of the image. Considerable latitude is available, in terms of placement, size and intensity to blend the watermark into a graphic.*

Another spatial watermarking technique uses color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. However, the watermark appears immediately when the colors are separated for

printing. This renders the document useless to the printer unless the watermark can be removed from the color band. This approach is used commercially for journalists to inspect digital pictures from a photo-stockhouse before buying un-watermarked versions.

An alternative to spatial watermarking is frequency domain. In this case, transforms like the Fast Fourier Transform (FFT) alter the pixel-values of the image for chosen frequencies. Since high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies that contain important information of the original picture (feature-based schemes). Since watermarks applied to the frequency domain will be dispersed over the entirety of the spatial image upon inverse transformation, this method is not as susceptible to defeat by cropping as the spatial technique. However, there is more of a tradeoff here between invisibility and decodability, since the watermark is in effect applied indiscriminately across the spatial image.

Watermarking can be applied to text images as well. Three proposed methods are: text line coding, word space coding, and character encoding. For text line coding, the text lines of a document page are shifted imperceptibly up or down. For a 40-line text page, for instance, this yields 2^{40} possible codewords. Figure 3a illustrates text line coding as it would appear to the casual reader. According to the line code box, the first, second, fourth and sixth lines are elevated by 1 pixel, although the alteration is practically imperceptible. The effectiveness of such watermarking is confirmed in Figure 3b. Even with the affected lines set apart in red, it is still difficult to determine that the lines are elevated.

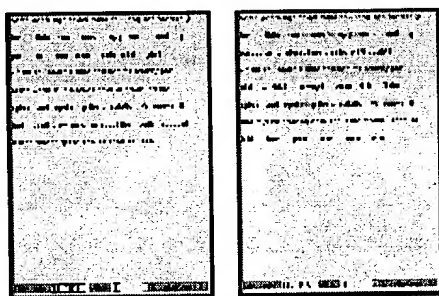


Figure 3a. Text with lines 1, 2, 4 and 6 elevated from normal position by 1 pixel.

Figure 3b. Elevated lines highlighted.

For word-shift coding, the spacing between words in a line of justified text is altered. The plaintext in Figure 4a has three words shifted right one pixel. Figure 4b highlights the affected words.



Figure 4a. Text with three words offset by one pixel.

Figure 4b. Text with offset words highlighted.

The remaining text watermarking technique involves character coding. This involves minor alterations to the shapes of characters - e.g., clipping a serif imperceptibly, or extending a descender. An advantage of these methods over those applied to picture images is that, by combining two or three of these to one document, two documents with different watermarks cannot be spatially registered to extract the watermark. Of course, the watermark can be defeated by retyping the text.

LIMITATIONS OF DIGITAL WATERMARKING

As of this writing, a counterfeiting scheme has been demonstrated for a class of invertible, feature-based, frequency domain, invisible watermarking algorithms. This counterfeiting scheme could be used to subvert ownership claims because the recovery of the digital signature from a watermarked image requires a comparison with an original. We may illustrate the point simply with graphics.

Standard watermarking involves the creation of a watermarked image by encoding a signature into an original image. Authentication proceeds in two stages. First, the watermark's signature is "removed" from the watermarked copy. The watermark signature is the "difference" between the original (white) and the watermarked copy of the original (blue). Next, the extracted signature (blue) is compared against the original signature (gold). Identity signifies authenticity of the copy.

*Figure 5a. Basic Watermarking technique.**Figure 5b. Watermark "inversion" for counterfeiting.**Figure 5c. Counterfeit logic.*

The counterfeiting scheme (see Figure 5b) works by first creating a counterfeit watermarked copy (violet) from the genuine watermarked copy (blue) by effectively inverting the genuine watermark. This inversion produces a counterfeit signature (violet) as well.

The trick is that the original image and bonafide signature stand in the same relationship to the watermarked image as the counterfeit image and counterfeit signature (see Figure 5c). Thus, the technique of establishing legitimate ownership by recovering the signature watermark by comparing a watermarked image with the original image breaks down. While it may be demonstrated that at least one recipient has a counterfeit watermarked copy, it can not be determined who it is.

This research suggests that not all watermarking techniques will be useful in resolving ownership disputes in courts of law. There will likely be non-commercial applications, or those with limited vulnerability to theft, where "good enough watermarking" will suffice. More sensitive applications may require non-invertible or non-extracting watermarking techniques. These issues are under consideration at this writing.

THE FUTURE OF WATERMARKING

The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to protect such interests. Though much research remains before watermarking systems become robust and widely available, there is much promise that they will contribute significantly to the protection of proprietary interests of electronic media. Collateral technology will also be necessary to automate the process of authentication, non-repudiable transmission and validation.

FOR FURTHER READING:

Some of this material was adapted from Berghel, H. and L. O'Gorman, "Protecting Ownership Rights through Digital Watermarking," IEEE Computer, 29:7, pp. 101-103 (1996). A good overview of how counterfeiters could "attack" watermarked images based on the correlation of the differences between samples is reported in Stone, H., "Analysis of Attacks on Image Watermarks with Randomized Coefficients," NEC Research Institute Technical Report, May 17, 1996. The counterfeiting scheme described here will appear in Craver, S., N. Memon, B. Yeo, and M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications," IEEE Journal on Selected Areas of Communications, December, 1997. The latter two papers also contain useful references to the watermarking literature. Information on IBM's digital library project (e.g., Figure 1) is to be found at <http://www.ibm.com/IBM/ibmgives/diglib.htm>. The images in Figures 2a through 3b were taken from our digital watermarking demonstration program which is available as freeware for non-commercial use through the author's ftp site (see homepage URL, below).

Hal Berghel is a professor of computer science at the University of Arkansas and a frequent contributor to the literature on cyberspace. He may be found (virtually) at www.acm.org/~hlb/.